AUGUST 2023

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our August 2023 Counter Fraud newsletter for NHS staff. We hope you find the contents helpful. If you need any advice on fighting NHS fraud, you can find our contact details on the final page.

IN THIS EDITION

HMRC advice on tax avoidance schemes

HMRC have warned that some NHS workers, mostly physiotherapists, radiographers, nurses and social workers have been targeted by intermediaries offering tax relief on earnings.

These schemes may seem to be legitimate and can be tempting, but they do not work and the tax will remain due.

Disguised Renumeration (DR) is the most common scheme of this type. It usually involves payment being made as a loan rather than a salary. A loan is non taxable and so payment to the HMRC would not be expected. However, because there is no intent to repay the money, it is not a loan and therefore it is income on which tax is due.

Many healthcare workers have been duped into such a scheme and they now face huge tax bills.

Further information can be found on the GOV.UK website: Tax avoidance – don't get caught out

Victim Describes Harrowing AI Kidnap Scam

In the April edition of this newsletter we featured an article about how Artificial Intelligence could be used to carry out more sophisticated fraud.

We have also included several articles about the "Hi Mum / Hi Dad" WhatsApp scam in which a fraudster impersonates their victim's children and claim to be in need or urgent assistance.

A victim of an Artificial Intelligence kidnapping scam has described her experience in the Guardian this month. The scam was a more sophisticated and upsetting variation on the theme of impersonating family members.

The fraudsters used AI to recreate the voice of the victim's daughter, and used this to cause alarm and distress in an attempt to blackmail her for a large sum of money. The description given by the victim is very impactful and sheds light on the potential methodologies that can be used.

To read the full account, please visit the Guardian website.
Please note the article contains distressing content where the threats made by the fraudster are described.

Scam Trends

Fake Fuel Card Offers

Which? have reported that emails and social media posts about fake fuel card offers are doing the rounds again. This scam was popular about a year ago.

The offer is to receive a free or discounted fuel card entitling the motorist to up to 200 litres of fuel from a company such as BP.

If a person clicks on a link to enter the competition or receive the offer, they are taken to a fake website.

If they put their details in, these are harvested and used by the fraudster.

Advice

Be wary that scammers can, and do, impersonate big companies. If the offer seems too good to be true, it is probably a scam.

Go to the company website – they will advertise their own offers. If it isn't advertised there, it is likely to be a fake.

More details on how the scam works and what it looks like on social media can be found on the Which? website.

Social Media Hijackers

A recent article on the This is Money site highlighted a social media scam exploiting people's trust in small businesses.

The scammers targeted Julie Ashworth, who runs a successful business mostly via Instagram. They convinced her that she needed to "secure her account" and tricked her into sharing her log in details.

They locked her out of her account and messaged her customers using her profile. They told her followers that they were at risk of being hacked too, and directed them to follow the same process that had been used to steal her account. Similar tactics are used to encourage social media users to engage in fake investment scams, taking advantage of people's increased trust in figures they follow or engage with on these platforms.

Advice

- Protect social media accounts with strong, unique passwords.
- Where it is available, turn on Multi Factor / Two Step Authentication. This option is usually found in the Security or Privacy section of the app settings.
- Be wary of emails or direct messages claiming you are at risk and need to click on links or follow instructions. Watch out for fake investment scams or requests for money or your personal / sensitive information.
- If you are concerned that your account may be at risk, go into the security settings of the app and change your password / activate Multi Factor / Two Step Authentication.

Scam Call Impersonating the NHS

The Counter Fraud Team have been made aware of a scam call which was made to a patient in Yorkshire.

The fraudster claimed to be from the NHS and said they were calling to confirm the patient's appointments. They asked for the patient's name, address, date of birth, national insurance number, and bank details.

When the patient refused to share their bank details, the caller stated that all of their appointments would be cancelled and ended the call.

The patient attended their local hospital where they were reassured that their appointments had not been cancelled.

Advice

- NHS services will not ask you to share your bank details over the phone.
- If you receive an unexpected call asking you to share personal information to "confirm your identity", end the call. Wait 30 minutes or use a different phone to call the organisation back on an official contact number to verify if the call was genuine.
- We advise waiting 30 minutes or using a different phone because some fraudsters can jam your phoneline. Even though you think you've hung up, they are still on the line and will intercept your next outgoing call.
- Don't rely on your caller display - fraudsters can disguise their number using spoofing software.

Cyber Fraud - Using QR Codes Safely

If you read the York Press you may have seen a feature recently about fraudsters posting QR codes in car parks in York city centre. When the codes were scanned, instead of taking the drivers to a site to pay for their parking, it took them to a site controlled by fraudsters who took the car parking fee – and then continued to make debits every day until it was cancelled.

What are QR Codes?

A QR code is simply a shortcut to accessing a website. They are increasingly being used by many businesses. For example, some restaurants no longer have a paper menu, instead they provide a QR code which visitors scan to view the menu, place orders, and pay for their meal. During the Covid-19 pandemic this was a particularly popular tool for shops and other services which was used to limit the number of surfaces customers needed to touch.

To use a QR code, open your camera app on your phone and point it at the code. Your camera will detect the site the code is linked to and you can see which internet address it will take you to. If you are happy to continue, you simply press the link which will have appeared.

The QR code itself cannot be hacked, the fraud risk is in relation to the site the code leads you to.

The Counter Fraud Team have their own QR code which is linked to our website - audityorkshire.nhs.uk. If you want to practice, have a go at scanning our QR code and see what you think.

In short, QR codes are a great way to quickly access information and the majority are legitimate. However, other than using them to check what you will be having for dinner, or reading back issues of the counter fraud newsletter, please stop and think before you enter information into websites which have been accessed via a QR code. If in doubt, look for alternative ways to contact the company.

If you are planning on parking in York, please note that payment is by cash or card at the on site machines, or via a parking app accessible on your mobile phone.

NEW TO QR CODES?

Please feel free to try scanning our QR code. It will take you to our website where you can find previous editions of this newsletter. We promise we won't ask for any personal info or bank details!.

Advice

• Look at the QR code before you scan it to make sure that a sticker hasn't been placed over the top.

• Use the camera app on your phone to scan codes – you do not need to download a QR app.

• Check the internet address the code wants to take you to. Once you are in the website, it may look legitimate, but the address (URL) will not match the official website in suspicious cases.

• If you have accessed a website through a QR code, don't put any financial details, personal information or username / passwords into the site it has taken you to.

• If you receive an email with a QR code telling you to access this to make a payment, double check with the company or access their website in a new browser.

You can find more information and advice on the Credo website.

In the Press

Man facing £100k bill and Contempt of Court Proceedings after Suspicious Compensation Claim

Sean Murphy had surgery for a torn bicep tendon in 2017, and during the operation his elbow was damaged. Sean claimed that this injury had left him unable to work, go to the gym or play rugby, and that he was dependent on his wife to help him get dressed. He sought compensation of £580,000 from the NHS.

However, a tip-off was then received that Murphy had been dishonest when describing the extent of the impact on his day-to-day life. Solicitors pointed to evidence including videos on his Facebook account which appeared to show him lifting very heavy weights. They also noted that he had returned to work laying decking and tarmac, and that local media coverage of rugby matches included his name in the line up.

Judge James Healy-Pratt dismissed Murphy's claim and he has been ordered to pay back £50,000 in compensation that he had already been paid. He also faces having to pay the legal costs of the NHS, with the total bill looking to be over £100,000.

Murphy continues to argue that his claim was not dishonest. A further trial for contempt of court proceedings is due to take place. You can read more on the Metro website.

Fraud Prevention Masterclasses

The 2023/24 Fraud Prevention Masterclass programme has now launched. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. Further dates will be published later this year. We will be covering the following topics:

General Fraud Awareness	23rd October 11am
Fraud Awareness for Managers	14th September 10am, 1st November 10am
Cyber Fraud	25th October 10am
Payroll Fraud	8th September 11am, 9th November 2pm
Procurement Fraud	24th October 10am
Creditor Payment Fraud	12th September 11am, 13th November 11am
Fraud Awareness for HR	5th October 2pm
Recruitment Fraud	28th September 2pm, 16th November 2pm

If you'd like to book a place for any of these sessions, please contact yhs-tr.audityorkshire@nhs.net

Bespoke Training Sessions

The Local Counter Fraud Team are always happy to pop along to speak to individual teams. If you would like us to attend one of your team meetings, to deliver a training session on a key fraud risk area, or for any other fraud prevention advice, please contact us using our details (which you'll find on the last page).

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details on the next page.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number. You'll find these details on the next page.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details are on the next page.

CONTACT US

Acronym Decoder
LCFS - Local Counter Fraud Specialist
LSMS - Local Security Management Specialist
ICB - Integrated Care Board

Steve Moss
Steven.Moss@nhs.net / 07717 356 707

Head of Anti Crime Services / LCFS

Steve manages the Counter Fraud Team.

Marie Dennis (was Hall)
Marie.Dennis2@nhs.net / 07970 265 017

Assistant Anti Crime Manager covering all clients, and LCFS covering:

York and Scarborough Teaching Hospitals NHS Foundation Trust

NHS Professionals

Nikki Cooper
Nikki.Cooper1@nhs.net / 07872 988 939

LCFS Covering:
Humber Teaching NHS Foundation Trust

Humber and North Yorkshire ICB

Leeds Community Healthcare

Rosie Dickinson
rosie.dickinson1@nhs.net / 07825 228 175

LCFS Covering:
Harrogate and District NHS Foundation Trust

Spectrum Community Health CIC

West Yorkshire ICB

Shaun Fleming
ShaunFleming@nhs.net / 07484 243 063

LCFS and LSMS Covering:

Calderdale and Huddersfield NHS Foundation Trust

West Yorkshire ICB

Lincolnshire ICB

Rich Maw
R.Maw@nhs.net / 07771 390 544

LCFS Covering:

Bradford Teaching Hospitals NHS Foundation Trust

Local Care Direct

Mid Yorkshire Teaching NHS Trust

Lee Swift
Lee.Swift1@nhs.net 07825 110 432

LCFS Covering:
Airedale NHS Foundation Trust
AGH Solutions
Bradford District Care NHS Foundation Trust
Leeds and York Partnership NHS Foundation Trust

You can also report fraud concerns to the NHS Counter Fraud Authority:
0800 028 40 60
https://cfa.nhs.uk/reportfraud

Follow us on Twitter - search for @AYCounter Fraud

Scan here to see previous editions of our newsletters